Final Report for Period: 10/2007 - 09/2008	**Submitted on:** 12/19/2008
Principal Investigator: Ahamad, Mustaque .	**Award ID:** 0121643

Organization: GA Tech Res Corp - GIT

Submitted By:
Ahamad, Mustaque - Principal Investigator

Title:
ITR/SI: Guarding the Next Internet Frontier: Countering Denial of Information

Project Participants

Senior Personnel

Name: Ahamad, Mustaque
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Omiecinski, Edward
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Pu, Calton
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Mark, Leo
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Liu, Ling
Worked for more than 160 Hours: Yes
Contribution to Project:

Post-doc

Graduate Student

Name: Bhatti, Yasser
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Koh, Younggyun
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Manivel, Vinay
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Singaravelu, Lenin
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Widener, Patrick

Worked for more than 160 Hours: No

Contribution to Project:

Name: Xiong, Li

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Zhan, Zhiyuan

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Huang, Weiyun

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Jun, Seung Won

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Liang, Gang

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Gupta, Vivek

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Deepak, Manohar

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Singh, Aameek

Worked for more than 160 Hours: Yes

Contribution to Project:

Aameek has worked on trust models with Co-PI Liu for peer-to-peer systems which are quite relevant for associating trustworthiness with sources of information.

Name: Viswanath, Ramesh

Worked for more than 160 Hours: Yes

Contribution to Project:

Mr. Viswanath is working on how to deal with entities that may not be fully cooperative with PI Ahamad.

Name: Webb, Steve

Worked for more than 160 Hours: Yes

Contribution to Project:

Mr. Webb has been working on the effectiveness of Bayesian filters for spam with Co-PI Pu.

Name: Wei, Jinpeng

Worked for more than 160 Hours: Yes

Contribution to Project:

Mr. Wei is a graduate research assistant who is working with Co-PI Pu.

Name: Yan, Wenchang

Worked for more than 160 Hours: Yes

Contribution to Project:

Mr. Yan is a graduate research assistant on the project and works with Co-PI Pu.

Name: Chitti, Subramanyan

Worked for more than 160 Hours: Yes

Contribution to Project:

Mr. Chitti participated in the project as a graduate research assistant and explored the application of learning techniques for countering denial of information (DoI) attacks.

Undergraduate Student

Technician, Programmer

Name: Sar, Vireak

Worked for more than 160 Hours: No

Contribution to Project:

Mr. Sar has been working on building basic support that could be used by this project.

Other Participant

Name: Zhou, Dong

Worked for more than 160 Hours: Yes

Contribution to Project:

Dr. Zhou spends 50% of his time on this project. He has been exploring the mailbomb attack and how it can be countered.

Name: Li, Kang

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Lee, Wenke

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Santos, Andre DoS

Worked for more than 160 Hours: Yes

Contribution to Project:

Research Experience for Undergraduates

Organizational Partners

Other Collaborators or Contacts

Activities and Findings

Research and Education Activities: (See PDF version submitted by PI at the end of the report)

The original end date of this project was 9-30-2006. A one year no-cost extension was approved in 2006. The project was in a wrap-up mode in 2006-2007 and all of the provided funds were expended before 9-30-2007. Results of the research completed by the PI, CoPIs and the graduate research assistants supported by the project were documented in the progress report that was submitted and approved in 2007.

We requested a second one year extension for this project in 2007 because of a supplemental award that was made to Georgia Institute of Technology to host the 2007 Cyber Trust PI meeting. Although we had estimated the cost of hosting this meeting as accurately as possible, there were left over funds from the supplemental award after covering all costs associated with the PI meeting. After consulting with NSF program managers, we decided to use them to support research agenda setting type workshops. The second extension allowed us to use the funds to host one such workshop on sensor and wireless security in April 2008. This was attended by approximately two dozen leading researchers in these fields. Professor Wenke Lee, one of the CoPIs of this project, was co-chair of the workshop program committee.

Since no research funds were available for personnel time or other similar activities in the past year, the 2007 report provides a complete description of the results of this project.

Findings: (See PDF version submitted by PI at the end of the report)

Training and Development:

Outreach Activities:

Journal Publications

Li Xiong and Ling Liu., "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communitie.", IEEE Transactions on Knowledge and Data Engineering (Special Issue on Peer to Peer Data Management)., p. 843, vol. 16, (2004). Published,

Greg Conti and Mustaque Ahamad, "A Taxonomy and Framework for Countering Denial-of-Information Attacks", IEEE Security and Privacy, p. , vol. , ( ). Accepted,

G. Conti, K. Abdullah, J. Grizzard, J. Stasko, J. Copeland, M. Ahamad, H. Owen and C. Lee, "Countering Security Analyst and Network Administrator Overload Through Alert and Packet Visualization", IEEE Computer Graphics and Applications (CG&A), p. , vol. , (2006). Published,

Li Xiong, Subramanyam Chitti, and Ling Liu, "Protecting Data Privacy in Outsourcing Data Aggregation Services", ACM Transactions on Internet Technology (Special Issue on the Internet and Outsourcing), p. , vol. , (2007). Accepted,

Bugra Gedik and Ling Liu, "Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms", IEEE Transactions on Mobile Computing, p. , vol. , (2007). Accepted,

Books or Other One-time Publications

M. Ahamad, W. Lee, L. Liu, L. Mark, E. Omicieski, C. Pu and A. dos Santos, "Guarding the Next Internet Frontier: Countering Denial-of-information Attacks", (2002). Book, Submitted
Collection: Proc. New Security Paradigms Workshop
Bibliography: none

M. Covington, P. Fogla, Z. Zhan and M. Ahamad, "A Context-aware Security Architecture for Emerging Applications", (2002). Technical Report, Published
Bibliography: Georgia Tech Technical report

Kang Li and Zhenyu Zhong, "Resisting SPAM Delivery by TCP Damping", (2004). Conference, Accepted
Collection: Proc.of First Conference on Email and Anti-Spam (CEAS)
Bibliography: None

Kang Li, Francis Chang, Damien Burger, and Wu-chang Feng., "Architecture for Packet Classification Caching", (2003). Conference, Published
Collection: Proceedings of IEEE International Conference On Network (ICON) 2003
Bibliography: None

Li Xiong and Ling Liu, "A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities", (2003). Conference, Published
Collection: In Proceedings of the 2003 IEEE Conference on E-Commerce (CEC'03)
Bibliography: None

Aameek Singh and Ling Liu, "TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P networks", (2003). Conference, Published
Collection: Proceedings of IEEE International Conference on Peer to Peer Computing. (IEEE Press).
Bibliography: pp142-149, Oct/November, 2003.

Huang, Weiyun; Omiecinski, Edward; and Mark, Leo, "Differential Stream Clustering on Categorical Data", (2003). Technical Report, Published
Collection: Tech Report, GIT-CC-03-13 College of Computing, Georgia Institute of Technology.
Bibliography: None

Huang, Weiyun; Omiecinski, Edward; and Mark, Leo, "Evolution in Data Streams", (2003). Technical Report, Published
Collection: Tech Report, GIT-CC-03-14. College of Computing, Georgia Institute of Technology.
Bibliography: None

Mudhakar Srivatsa, Li Xiong and Ling Liu., "SGuard: Dependable Reputation Management System for Large Scale Distributed Systems.", ( ). Conference, Submitted
Bibliography: None.

Sunkeun Park, Ling Liu and Calton Pu, "Attack Resistant Trust Management in Decentralized Peer to Peer Systems.", ( ). Conference, Submitted
Bibliography: None.

Oleg Kolesnikov, Wenke Lee and Richard Lipton, "Filtering Spam Using Search Engines.", ( ). Conference, Submitted
Bibliography: None.

Greg Conti and Kulsoom Abdullah, "Passive Visual Fingerprinting of Network Attack Tools", ( ). Workshop, Submitted
Bibliography: None.

Michael Covington, Mustaque Ahamad, Irfan Essa and H. Venkateswaran, "Parameterized Authentication.", (2004). Conference, Accepted
Collection: 9th European Symposium on Research in Computer Security.
Bibliography: None.

Steve Webb and Calton Pu, "An Experimental Evaluation of Bayesian Filter Effectiveness and Resistance Against Attacks in Spam Filtering", ( ). Conference paper, In preparation.
Bibliography: None.

G. Conti, M. Ahamad and J. Stasko, "Attacking Information Visualization System Usability: Overloading and Deceiving the Human", (2005). Conference Proceedings, Accepted
Collection: Symposium on Usable Privacy and Security (SOUPS)
Bibliography: none

G. Conti, M. Ahamad and R. Norback, "Filtering, Fusion and Dynamic Information Presentation: Towards a General Information Firewall", (2005). Conference Proceedings, Published
Collection: IEEE International Conference on Intelligence and Security Informatics (IEEE-ISI)
Bibliography: none

W. Huang, E. Omiecinski and L. Mark,, "Compression Schemes for Differential Categorical Stream Clustering", (2004). Conference Proceeding, Published
Collection: 13th ACM International Conference on
Information and Knowledge Management
Bibliography: none

J. Li and E. Omiecinski, "Efficiency and Security Trade-off in Supporting Range Queries on Encrypted
Databases", (2005). Conference Proceedings, Accepted
Collection: 19th IFIP Working Conference on Data and
Applications Security
Bibliography: none

Mudhakar Srivatsa and Ling Liu, "Countering Targeted File Attacks using LocationGuard", (2005). Conference Proceedings, Accepted
Collection: 14th USENIX Security Symposium (USENIX Security)
Bibliography: none

Bugra Gedik, Ling Liu, "A Customizable k-Anonymity Model for Protecting Location Privacy", (2005). Conference Proceedings, Published
Collection: International Conference on Distributed Computing Systems
Bibliography: none

Mudhakar Srivatsa, Li Xiong and Ling Liu., "TrustGuard: Countering Vulnerabilities in Reputation Management For Decentralized Overlay Networks", (2005). Conference Proceeding, Published
Collection: 14th World Wide Web Conference (WWW 2005)
Bibliography: none

Aameek Singh, Kaladhar Voruganti, Sandeep Gopisetty. David Pease, Linda Duyanovich and Ling Liu, "Security vs Performance: Tradeoffs using a Trust Framework", (2005). Conference Proceedings, Published
Collection: 22nd IEEE-NASA Conference on Mass Storage Systems and Technologies (MSST)
Bibliography: none

Li Xiong and Ling Liu, "Reputation and Trust in Mobile Commerce", (2005). Book, Published
Collection: Advances in Security and Payment Methods for Mobile Commerce
Bibliography: Idea Group Inc.

Mudhakar Srivatsa and Ling Liu, "Vulnerabilities and Security Threats in Structured Overlay Networks: A Quantitative Analysis", (2004). Conference Proceedings, Published
Collection: 20th Annual Computer Security Applications Conference (ACSAC 2004)
Bibliography: none

Sungkeun Park, Ling Liu, Calton Pu, "Resilient Trust Management for Web Service Integration", (2005). Conference Proceedings, Published
Collection: 3rd IEEE International Conference on Web Services (ICWS 2005)
Bibliography: none

Steve R. Webb, Subramanyam Chitti, and Calton Pu, "Attack-Resistant Spam Filter Design and Evaluation", ( ). Conference Proceedings, Submitted
Bibliography: none

Seung Jun, Mustaque Ahamad and Jun Xu, "Robust Information Dissemination in Uncooperative Environments", (2005). Book, Published
Collection: International Conference on Distributed Computing (ICDCS)
Bibliography: none

James Caverlee and Ling Liu, "Countering Web Spam with Credibility-Based Link Analysis", (2007). Conference paper, Published
Collection: The 26th ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC) 2007
Bibliography: Portland, OR

Mudhakar Srivatsa and Ling Liu, "Secure Event Dissemination in Content-Based Publish-Subscribe Networks", (2007). Conference paper, Published
Collection: Proceedings of 27th IEEE International Conference on Distributed Computing Systems
Bibliography: None

Aameek Singh, Mudhakar Srivatsa, Ling Liu, "Efficient and Secure Search of Enterprise File Systems", (2007). Conference paper, Published
Collection: Proceedings of IEEE International Conference on Web Services
Bibliography: None

James Caverlee, Steve Webb, and Ling Liu, "Spam-Resilient Web Rankings via Influence Throttling", (2007). Book, Published
Collection: Proceedings of the 21st IEEE International Parallel and Distributed Processing Symposium (IPDPS)
Bibliography: None

Aameek Singh, Ling Liu, Mustaque Ahamad, "Privacy Analysis for Data Sharing in *nix Systems", (2006). Conference paper, Published
Collection: USENIX Annual Technical Conference
Bibliography: None

L. Xiong, S. Chitti and L. Liu, "Mining Multiple Private Databases using a Privacy Preserving kNN Classifier", (2006). Conference paper, Published
Collection: 15th ACM Conference on Information and Knowledge Management (CIKM)
Bibliography: None

Steve Webb, J. Caverlee, and C. Pu, "Characterizing Web Spam Using Content and HTTP Session Analysis", (2007). Conference paper, Published
Collection: Proceedings of the Fourth Conference on Email and Anti-Spam
Bibliography: None

B. Byun, C. Lee, Steve Webb, and C. Pu, "Discriminative Classifier Learning Approach to Image Modeling and Spam Image Identification", (2007). Conference paper, Published
Collection: Proceedings of the Fourth Conference on Email and Anti-Spam
Bibliography: None

Web/Internet Site

URL(s):

http://www-static.cc.gatech.edu/projects/doi/WebbSpamCorpus.html

Description:

This site provides the research community access to web spam data that can be used to evaluate a variety of techniques that are being developed for combating denial of information attacks.

Other Specific Products

Contributions

Contributions within Discipline:

Contributions to Other Disciplines:

Contributions to Human Resource Development:

Contributions to Resources for Research and Education:

Contributions Beyond Science and Engineering:

Categories for which nothing is reported:

Organizational Partners
Activities and Findings: Any Training and Development
Activities and Findings: Any Outreach Activities
Any Product
Contributions: To Any within Discipline
Contributions: To Any Other Disciplines
Contributions: To Any Human Resource Development
Contributions: To Any Resources for Research and Education
Contributions: To Any Beyond Science and Engineering

Findings

A summary of our findings for the various activities is presented below.

Countering Information Visualization Attacks: Information visualization systems used for decision making must be designed with security in mind. In particular, they must highlight good quality information and should hide noise to reduce the impact of DoI attacks. Information visualization systems are vulnerable to attack, either from malicious entities attempting to overwhelm, mislead or distract the human viewer or from non-malicious entities that accomplish the same result by accident. Clearly there are many domains where information visualization systems are being used to support critical decision making. For example, intelligence analysis, law enforcement, network security and business decision-support systems exist in an adversarial environment where it is likely that malicious entities are actively attempting to manipulate human end users. To help combat usability attacks against visualization systems, this work includes several novel contributions: a framework for information visualization system security analysis, taxonomy of malicious attacks as well as technology independent principles for designing information visualization systems that will resist attack. We have illustrated and validated these contributions with results from the design, implementation and real-world use of a visual network intrusion detection system.

Information Firewall: The rate at which data is being produced, combined with the immense amount of existing data, sets the stage for denial of information attacks against both analysts and their customers. Denial of Information (DoI) attacks are similar to Denial of Service (DoS) attacks against machines. While DoS attacks attempt to deny users access to system resources by consuming machine resources, DoI attacks target the human by exceeding their perceptual, cognitive and motor capabilities. In most cases, a small amount of malicious information is all that is required to overwhelm or deceive the human. A successful DoI attack occurs when the human does or does not take action they otherwise would have. Denial of Information attacks are of critical importance to intelligence analysts. Every bit of time, albeit small, wasted on a false lead or due to information overload reduces the probability of timely and accurate action. To counter DoI attacks, we employed collaborative, knowledge-based user interfaces that improve data quality. These interfaces, based upon filtering, fusion and dynamic transformation techniques, reduce the amount of irrelevant data (noise) and increase the useful information (signal) presented to the analyst. An information firewall abstraction developed and implemented by us supports the following functions: (1) Filtering unneeded information based on shared experiences, (2) Fusing multiple information sources into a single consolidated page, (3) Transforming poorly designed information architectures and interfaces into far more usable ones, and (4) Sharing of transforms via simple techniques such as browsing an index or emailing a link to a colleague. A prototype of this system was developed.

Dependable Reputation Management System: Reputation-based trust models have been popular in estimating the trustworthiness and predicting the future behavior of nodes in a large-scale distributed system such as a Peer-to-Peer (P2P) file sharing network. One of the fundamental challenges in distributed reputation management is to develop mechanisms that can minimize the potential damages to the system by malicious nodes. In this area, we have obtained two major results. First, we have developed the PeerTrust model and system for evaluating and building trust among unknown peers within an open peer to peer online community. This work continues on top of the work reported in our last year's report. Second, we develop an attack resilient trust management system through TrustGuard, a three-tier safeguard framework and set of optimization techniques for providing a highly dependable and yet efficient reputation management system. Our experiments show that, comparing with existing reputation systems, our three-tier framework is highly dependable and effective in countering malicious nodes regarding strategic colluding or oscillating behavior, dishonest feedbacks, and flooding malevolent feedbacks with fake transactions. Several extensions to the PeerTrust research are undergoing, including the effort made to extend the trust framework to manage large distributed data systems and the work on handling vulnerabilities due to sparse votes in reputation based trust management system.

SGuard: Security Guards for Large Scale Overlay Networks: Peer to peer communities connected by overlay networks will increasing facilitate information publishing and access. Overlay networks are virtual networks constructed on top of a typical TCP/IP network comprising of 1000s of nodes. These large scale distributed systems pose several interesting problems with respect security, reliability and performance. SGuard project is aimed at building security guards for such large scale distributed systems against various security threats, including DoS and DOI attacks, while maintaining acceptable system performance. In this research, we have developed several algorithms to address the challenges faced in creating secure and efficient overlay networks. First, we identified three important vulnerabilities and security threats in application independent overlay networks and proposed countermeasures against them. Second, we developed TrustGuard, a secure and efficient reputation management system for overlay networks. As a part of TrustGuard, we developed XChange, a Byzantine fault-tolerant protocol for performing electronic fair-exchange. We call it the ExchangeGuard. Third, we developed LocationGuard, to efficiently hide the location of resources (files and objects) on an overlay network. LocationGuard uses location keys for obfuscating the location of a file on the overlay network such that only a legal user of the file can locate the file on the overlay network. As a part of LocationGuard, we are developing SWANFS a secure distributed file system that uses location keys to guard files from denial-of-service and host compromise attacks.

Protecting Data Privacy in Large Scale Distributed Applications: This is a new research initiative related to the DoI project, aiming at countering denial of information attack through building privacy-aware applications and middleware. As we know DoI attacks focus on making the information unavailable for timely access. Another potential threat of DoI is the violation of confidentiality and integrity of information such that attackers can use private information to issue DoI attacks to mission-critical applications. Through the study of data privacy issues, we also identify several privacy related DoI attacks such as Denial of information attack using leaked private Identity information or pseudo identity information, and denial of information attack using location data. This research emphasizes the importance of data privacy against DoI attacks in large scale pervasive computing environment. Several ongoing research efforts are along this direction. First, we are working on mechanisms for countering vulnerabilities exhibited in current file management systems. Second, we are working on geometric perturbation techniques for protecting data privacy in large scale data sharing and data outsourcing

Effectiveness of Spam Filtering: We have made significant progress in the spam filter evaluation project. We have expanded our investigation of the effectiveness of Bayesian filters to include Support Vector Machines (SVM) and Logit Boost, the three main statistical learning techniques with applicability to problems such as spam identification. We have used public archives of known spam messages and known legitimate (non-spam) messages in the training of these filters. Our initial hypothesis is that adaptive learning techniques are vulnerable to Denial-of-Information attacks. This hypothesis has been verified. We proceeded to examine the problem of "arms race" between our learning filters and adaptive spammers who are trying to get around the learning filters. The existence of arms race has been verified, too. Our recent result shows that, perhaps contrary to intuitive expectations, the arms race does not have to go on forever. There are techniques capable of overcoming the arms race problem for specific domains such as spam identification.

Reducing Noise in Event Log Collection: It is well known that event logs are very effective tools in applications such as intrusion detection and problem diagnosis. However, the trade-off between high level events (that do not help very much in analysis) that carry little overhead and low level events (that contain useful information for analysis) that carry significant monitoring and storage overhead has been a road block in the wide adoption of this approach. One could describe this problem as a self-denial-of-information, since the noise is introduced by the monitoring system itself. In our investigation of searching for interesting kernel events, we have applied our knowledge of denial-of-information problems to reduce monitoring noise by analyzing events online and adaptively changing the monitoring level according to need. During this past year, the focus of this effort has been in the domain of TOCTTOU (Time of Check To Time of Use) vulnerabilities. We have developed a model of TOCTTOU and techniques to find them and guard against them. The evaluation of event logs and denial of information issues will be investigated further this year with TOCTTOU as an illustrative domain.

Data Change Management: From our perspective, if information quality such as accuracy, timeliness or credibility is compromised, then it is equivalent to a denial of information. Typical integrity constraint mechanisms, such as those provided by current database management systems, are only a part of guaranteeing data quality. An important part of ensuring data quality is the task of monitoring the changes that are taking place on the data and how they affect the overall model of the data. To this end, we have worked on the following issues:

(1) We have formalized the change detection problem and have proposed several metrics to evaluate change detection. We have also devised a novel low-cost approach to detect changes of data models in data streams and have shown the advantages of our approach using subspace cluster monitoring.

(2) We have developed a new cluster-outlier detection algorithm. Our algorithm identifies outliers, data points that deviate from the norm, and also the cluster of data points for which a data point is considered to be an outlier. Our method also has the ability to rank the outliers based on the user defined level of interest. Our approach provides essential information for outlier detection analysis, which other approaches do not.

As a side issue, we also explored the use of different data encryption methods. With the data being encrypted it is less likely that unauthorized users will be able to read and corrupt the data values. We examined the security and efficiency tradeoff of the encryption techniques for relational database systems.

Information Dissemination in Uncooperative Environments: For reliable and timely delivery of information in a large scale system, we consider a multicast tree in which nodes are potentially uncooperative except the information source node, which is trusted by all other nodes. In this setting, some nodes will follow the protocol faithfully while others may be uncooperative. As a result of uncooperative behavior, for instance, messages can be illicitly modified or blocked on the way. In this work, we addressed the following question: *how can we provide efficient and reliable information dissemination to well-behaved nodes when the messages are relayed via possibly uncooperative nodes?* To address this question, we proposed Trust-Aware Multicast (TAM). TAM is designed to deliver data in a reliable and timely manner, even in the presence of uncooperative nodes in the system. We achieve this goal by detecting uncooperative behavior, evaluating nodes based on their behavior history, and adapting the multicast tree in such a way that more trusted nodes are located closer to the source node. In this way, the system becomes more robust over time. The property of TAM not only improves robustness but also facilitates deployment because the system admits any user without establishing a trust relationship beforehand. We emphasize the necessity of trust awareness as a design principle for emerging overlay and peer-to-peer applications, including information publishing and access in open systems.

Activities

We have continued to work on all aspects of the project. In the past year, we have focused on the following activities.

1. Quantitative evaluation of DoI attacks and defenses. In particular, we are evaluating the effectiveness of Bayesian and other filters against spam based DoI attacks.
2. Malicious visualization of network activity information. Visualization of information is one technique for enhancing the quality of information (QoI) which DoI attacks seek to degrade. We have explored how DoI attacks can target visualization techniques and have explored defenses against it. We have applied these techniques to information about network activity in a system.
3. Dependable reputation based systems for open peer-to-peer environments. Reputation or trust is one way to evaluate the quality of information that is accessed from a certain source. We are exploring robust and dependable techniques for associating reputation with peer nodes.
4. Protecting privacy of information in large scale systems. We identified several privacy related DoI attacks such as DoI attack using leaked private identity information or pseudo identity information, and DoI attacks using location data.
5. Working on the dynamic monitoring of Linux kernel events using CBE logs and event analyzer. The first concrete goal is to detect potential race conditions such as those exploited in TOCTTOU attacks.
6. Change detection techniques for data. From our perspective, if information quality such as accuracy, timeliness or credibility is compromised, then it is equivalent to a denial of information. Typical integrity constraint mechanisms, such as those provided by current database management systems, are only a part of guaranteeing data quality. An important part of ensuring data quality is the task of monitoring the changes that are taking place on the data and how they affect the overall model of the data. To this end, we have been working on the change detection problem.
7. Information dissemination in uncooperative environments. In open peer-to-peer systems, efficient information dissemination utilizes communication paths that could involve nodes that are not cooperative. We explored trust-aware communication structures for efficient dissemination of information.