1. Automated Reasoning about Web Access Control Policies via Answer Set Programming
   Gail-Joon Ahn*, Joohyung Lee*, Hongxin Hu and Yunsong Meng
   **Summary:** We introduce a logic-based policy management approach for XACML (eXtensible Access Control Markup Language), which has become the de facto standard for specifying and enforcing access control policies for various applications and services in current Web-based computing technologies. Our approach adopts Answer Set Programming (ASP) to formulate XACML that allows us to leverage the features of ASP solvers in performing various logical reasoning and analysis tasks, such as verifying policy properties and detecting violation of separation of duty (SoD) constraints in role-based access control (RBAC).

2. User Centric Identity Management for Online Social Networks (*with demonstration*)
   Gail-Joon Ahn* and Pradeep Sekar
   **Summary:** The current trends of social networks are indirectly requiring users to become system and policy administrators for protecting their content in cyber-enabled social settings. This is further complicated by the rapid growth rate of social networks and by the continuous adoption of new services on social networks, requiring more systematic user-centered access control. In addition, research has increasingly recognized the risk of misuse of personal data processed by online social networking applications and the lack of awareness among the user population. We discuss a comprehensive and compelling framework called SNGuard (Social Network Guard) that satisfies diverse privacy properties, access control issues, identity management requirements, and usage patterns.

3. Firewall Policy Analysis for Autonomic Computing
   Gail-Joon Ahn*, Hongxin Hu and Ketan Kulkarni
   **Summary:** The effectiveness of network-centric infrastructure protection provided by autonomic computing heavily depends upon the quality of network policies. Designing and managing different kinds of policies whether firewall policies or network configurations are often error prone due to the complexity of such network policies as well as the lack of effective analysis mechanisms and corresponding tools. Anomalies in a policy may result in security breaches or vulnerabilities. In this work, we demonstrate how firewall policies can be effectively analyzed and managed based on our framework that focuses on policy conflict detection & resolution and an intuitive visualization representation of analysis results.

* ASU faculty members
4. **RanKloud: Scalable, Information Utility Aware Data Processing in Server Clusters**
   K. Selcuk Candan*
   
   **Summary:** In many data analysis applications, the utility of a given data element to the particular analysis task depends on the way the data is collected (e.g. its precision) or interpreted. However, since existing parallel data processing frameworks do not consider variations in data utility, they are not able to focus on the best results. Even if the user is interested in obtaining a relatively small subset of the best result instances, these systems often need to enumerate entire result sets, even if these sets contain low-utility results. In this poster, we introduce RanKloud for processing ranked queries in batch-oriented cluster environments. Experimental results show that the proposed sampling, data partitioning, and join processing strategies enable results with high confidence and low-overhead (up to 9× faster than alternative schemes on 10 servers).

5. **Usable and Sustainable Security Solutions for Body Sensor Networks (with demonstration)**
   Ayan Banerjee, K.K. Venkatasubramanian, Tridib Mukherjee and Sandeep K. S. Gupta*
   
   **Summary:** The goal of this project is to provide usable (plug-and-play, self-configuring, and autonomic) and sustainable (operated with energy scavenged from human body) inter-sensor communication security for Body Sensor Networks (BSNs). Securing inter-sensor communication is required to maintain information privacy. In this regard we take a cyber-physical approach. We propose Physiological Value based Security (PVS) which achieves key agreement between two sensors in a BSN extracting common features from physiological signals sensed at the two sites. For sustaining the security protocol we consider energy scavenging from respiration, body-heat, ambulation and sunlight. We verify BSN sustainability through model based engineering.

6. **A location-based authentication using environment sounds for pervasive computing**
   Sandeep K. S. Gupta* and Su Jin Kim
   
   **Summary:** Pervasive computing is fast becoming a reality with rapid advance in computing and networking technologies. It has the characteristics of scalability, invisibility, and the absence of the fixed infrastructure. In many pervasive applications, devices collaborate with others within a particular area (such as a room or a building) and thus such applications need authentication for security. We propose a new authentication technique which allows devices to authenticate each other when they are within the same audio region. The main advantage of our scheme is that there is no need of the pre-shared secret, the pre-existing trust relationship and human involvement.

7. **Constructing Efficient Attribute-Based Broadcast Encryption**
   Dijiang Huang* and Zhibin Zhou
   
   **Summary:** Attribute Based Broadcast Encryption (ABBE) is a novel Broadcast Encryption (BE) approach. Compared to existing BE approaches that require an explicitly specified decrypters list, ABBE encrypter enforces an expressive access policy composed of one or more attributes. Although ABBE is more flexible and efficient with reduced storage overhead, ciphertext size of current ABBE schemes is linearly proportional to the numbers of attributes. In this paper, we investigate the solution on how to reduce the ABBE's ciphertext size to a constant value. Moreover, we explore the capability of using ABBE in secure many-to-many communication environments.
Dijiang Huang*, Yang Qin, and Zhibin Zhou  
**Summary:** We propose a new MANET infrastructure MobiCloud that transforms traditional MANETs into a new service-oriented communication architecture. Through a service-layered MobiCloud infrastructure, the MobiCloud trust management mechanism can address the interoperability issues effectively, and thus reduce the security setup uncertainty. To reduce the mobility uncertainty, we incorporate every SN as a virtualized component of the MobiCloud. MobiCloud mirrors a SN to one or multiple shadow images in the Cloud for addressing communication and computation deficiencies of mobile devices. Moreover, shadow images create a visualized MANET routing and communication layer that can maximally assist the mobile nodes to enable pervasive computing services for each mobile device owner.

Dijiang Huang*, Wei-Tek Tsai*, Aniruddha Kadne and Yongji Zhong  
**Summary:** We propose to develop a computer and network security instructional laboratory (CNS-IL) to enhance computer network security education. CNS-IL is designed to be a cost-effective, scalable, user-friendly, flexible, and remotely accessible virtual laboratory offering significant enhancements to undergraduate education in information assurance. CNS-IL incorporates the infrastructure/platform/software-as-a-service Cloud computing concept. These concepts are based on virtualization and clustering technologies that will maximally utilize existing computing and network resources for large-scale computer and network security based experiments. In addition to its technical merits, CNS-IL accomplishes a broader goal by introducing a number of versatile hands-on projects through a virtualized environment for student learning. The CNS-IL will be used in colleges, where students, particularly, undergraduates will work on fundamental security issues and technologies associated with computer and network technologies.

10. **Discriminative K-SVD for Dictionary Learning in Face Recognition**  
Baoxin Li* and Qiang Zhang  
**Summary:** Face recognition is an important modality of biometrics that has potentially wide application in identity management. We propose a method to learn an over-complete dictionary that has both representational capacity and discriminative power for sparse-coding based face recognition. The proposed method, discriminative K-SVD (D-KSVD), is based on extending the K-SVD algorithm by incorporating the classification error into the objective function, thus allowing the performance of a linear classifier and the representational power of the dictionary being considered at the same time by the same optimization procedure. The DKSVD algorithm finds the dictionary and solves for the classifier using a procedure derived from the K-SVD algorithm, which has proven efficiency and performance. Experiments with two large datasets show that the proposed method outperforms several competing methods in most cases.

11. **Mining Crowdsourced Data for Intelligent Decision Making**  
Geoffrey Barbier, Huiji Gao, Huan Liu*, and Xufei Wang  
**Summary:** Using social media tools and sites to share information and collect data is part of a broader trend called crowd-sourcing. An example is public-access crisis map, which is
publicly available and accessible for solving problems affecting choices in a crisis. Reports of trapped people, fires, polluted water sources, and requests for food, water and medical supplies are sent to the crisis map. The first respondents respond to these reports and requests based on their ability. With many organizations participating in major relief efforts, a shared or centralized information system is needed. We have designed an ASU Event Map (ASU-EMap) aiming to help the first responders in relief efforts. The reports in “Haiti Live” are re-organized into intuitive requirement categories and rendered on ASU-EMap with data mining technology.

12. Towards Building a Social Computing Tool for Social Scientists (with demonstration)
Shamanth Kumar and Huan Liu*
Summary: We have worked with social scientists and cultural anthropologists, and learned their ways of studying subjects in social media, what their needs are, and their interests. We have built a generic platform for collecting data in the blogosphere, tracking blogs of particular interests, and facilitating comparative data analysis. This poster presents and demonstrates a social computing tool that centers around social scientists, and show how we are inspired by the research of social scientists in our effort to build the platform - BlogTrackers, which can identify key topics of discussion, identify influential bloggers, track topics over time, and search blogs. These features can help social scientists to quickly analyze blogs and bloggers at a large scale.

13. SEAS: A secure and Efficient Anonymity Scheme for Low-Cost RFID tags
Guoliang Xue*
Summary: We present SEAS, a novel privacy preserving, anonymous authentication scheme for RFID tags, which allows the tags to use pseudonyms instead of their true identity for authentication. The pseudonyms do not reveal the identity of the tag and the pseudonyms of multiple authentications appear random and uncorrelated to the adversary. A pseudonym can only be deciphered by the backend authentication authority to identity the tag. No other entity in the network can link the pseudonym to the identity of the tag. We perform security analysis of our scheme to show its effectiveness against different forms of attacks.

14. Design of Adaptive Service-based Software Systems with Security and Multiple QoS Requirements (with demonstration)
Stephen S. Yau*, Nong Ye*, Hessam Sarjoughian*, Dazhi Huang, Ho An, Yin Yin, Mohammed Muqsith and Billibaldo Aranda
Summary: Managing QoS in service-based software systems (SBS) is needed, but challenging, due to their dynamic and loosely-coupled nature. In this poster, an overview of our approach to designing adaptive SBS (ASBS) with security and multiple QoS requirements is given. Our demonstration system based on voice communication, motion detection and encryption services will be used to illustrate our research results on dynamic resource allocation, QoS optimization based on genetic algorithms, handling the tradeoff among the QoS features of multiple workflows, and SOA-compliant simulation for applying our approach to larger SBS.

15. Confidentiality in Cloud Computing
Stephen S. Yau*, Gail-Joon Ahn*, Ho G. An
Summary: One of the major barriers to adopting cloud computing is the lack of security mechanisms customized for cloud-based transactions and services. In particular, supporting
confidentiality of users’ data is a common and critical services for cloud computing systems, but it has not been studied in depth. In this poster, we present an effective approach to protecting the confidentiality of users’ data processed and stored in cloud computing systems from unauthorized persons, processes or devices. We introduce two entities, Confidentiality Manager (CM) and Service Assurance Authority (SAA), in a cloud computing system: CM protects the confidentiality of users’ data at the system level and SAA protects the confidentiality of users’ data at the user level of a cloud computing system.

16. Tradeoffs of Service, Security and Attacks for Cyber System Survivability
   Nong Ye* and Billibaldo Martinez Aranda

   **Summary:** This poster presents our ongoing research on tradeoffs of service, security and attacks for cyber system survivability. When Cyber attacks cause unforeseen damage to a system, we expect the system to have the capability of dynamically adapting itself to survive and recover from damage. Dynamical adaptation requires tradeoffs within existing resources. A methodology is proposed to uncover cause-effect dynamics of services, security mechanisms and attacks on the state of system resources and QoS performance. These cause-effect dynamics can be used to determine how attacks compromise system resources and QoS performance and how service, security and system configurations can be adapted for system survivability under the damage of attacks.