5th Annual Workshop on
Information Assurance Research and Education

Information Assurance Center
Arizona State University

Posters and Demonstrations

Wednesday, April 25, 2012, 1:00 p.m. to 4:45 p.m.
Room 150, Artisan Court, Tempe, Arizona

1. **Usable Multi-party Control for Securing Social Networks** (with demonstration)
   Gail-Joon Ahn* and Hongxin Hu
   Summary: Online social networks (OSNs) have experienced tremendous growth in recent years and become a de facto portal for hundreds of millions of Internet users. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. In this project, we introduce comprehensive and compelling approaches to facilitate collaborative privacy management of shared data in OSNs. The resulting applications include MController, Retinue, and Sigma that focus on a voting-based solution, a risk-based approach and a circle-based management for data sharing, respectively. We also discuss our results of extensive usability studies and system evaluations of those applications.

2. **Towards Collaborative Forensics** (with demonstration)
   Gail-Joon Ahn* and Mike Mabey
   Summary: Digital forensic analysis techniques have been significantly improved and evolved in past decade but we still face a lack of effective forensic analysis tools to tackle diverse incidents caused by emerging technologies and the advances in cyber crime. We propose a comprehensive framework to address the efficacious deficiencies of current practices in digital forensics. Our framework, called Collaborative Forensic Framework (CUFF), provides scalable forensic services for practitioners who are from different organizations and have diverse forensic skills. In other words, our framework helps forensic practitioners collaborate with each other, instead of learning and struggling with new forensic techniques.

3. **Automatic Extraction of Secrets from Malware** (with demonstration)
   Gail-Joon Ahn* and Ziming Zhao
   Summary: As promising results have been obtained in defeating code obfuscation techniques, malware authors have adopted protection approaches to hide malware-related data from analysis. Consequently, the discovery of internal cipher text data in malware is now critical for malware forensics and cyber-crime analysis. In this work, we present an approach to automatically extract secrets from malware. Our approach identifies and extracts binary code relevant to secret hiding behaviors. Then, we relocate and reuse the extracted binary code in a self-contained fashion to reveal hidden information. We demonstrate the feasibility of our approach through a

* ASU Faculty Member

proof-of-concept prototype, called ASES (Automatic and Systematic Extraction of Secrets) along with experimental results.

4. **R2DB: A System for Querying and Visualizing Weighted RDF Graphs** (with demonstration)
Shengyu Huang, Xinsheng Li, Songling Liu, Juan P. Cedeno, K. Selcuk Candan*, and Maria Luisa Sapino
Summary: Increasingly, information systems need to be designed to help decision makers operate with imperfect knowledge, integrated from diverse sources. Existing data representation and query languages fail to support a large class of knowledge applications which associate utilities or costs on the available knowledge statements, thereby assuring the quality of the information provided to decision makers. Here, we introduce and demonstrate R2DB, a novel database system for querying weighted RDF graphs to assure accuracy of the information provided to the user. R2DB includes (a) a ranked RDF (R2DF) specification to enhance RDF triples with an application specific weights and (b) a SPARankQL query language specification, which provides novel primitives to express top-k queries using traditional query patterns as well as novel flexible path predicates. R2DB also provides an innovative features-of-interest (FoI) based method for visualizing large sets of query results.

5. **Cybercog: A Synthetic Task Environment for Studies of Cyber Situation Awareness**
Nancy Cooke*, Prashanth Rajivan, Shree Jariwala, and Michael Champion
Summary: This poster describes a synthetic task environment, called Cybercog, for controlled experiments using undergraduates. Synthetic task environments are abstractions of real tasks that provide a controlled environment for experimental research, yet preserves the critical aspects of the task. Cybercog is specifically for research on teams of cyber analysts and allows us to easily manipulate the situation, provides ground truth, and facilitates measurement of team situation awareness, accuracy and cognitive processing. We are currently redefining the task for a demonstration of the benefits of effective teamwork in the cyber domain. This work is supported by an ARO MURI grant (Cliff Wang, program manager).

6. **Usable and Sustainable Security Solutions for Body Sensor Networks**
Sandeep Gupta* and Priyanka Bagade
Summary: The main goal of this project is to provide usable (plug-and-play, self-configuring, and autonomic) and sustainable (can be operated from energy scavenged from the human body) inter-sensor communication security for Body Sensor Networks (BSNs). BSNs are often used in mission critical health monitoring and military applications and the constituent sensors deal with sensitive data. They transmit data through the wireless medium of communication which is open to security threats. Securing inter-sensor communication is thus a requirement to maintain the privacy of sensitive data. The security solution for BSNs should be plug-and-play – any new sensor plugged in to the BSN should start communicating securely without any initialization overhead (e.g. key pre-deployment, key exchange). This is an important requirement since security related initialization overhead can cause delay in deployment which can be harmful in time critical applications (such as in monitoring heart attack). Further, the security solution should be energy efficient so that it can be sustained through energy scavenged from human body. The BSN nodes are traditionally battery operated and are hence limited in lifetime. Security protocols drawing power from the node battery can further reduce the lifetime of a node.
To achieve a usable and sustainable security solution for BSN 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. We use Electrocardiogram (EKG) and Photoplethysmogram (PPG) signals to implement PVS in a BSN comprising of TelosB motes. For sustaining the security protocol we include energy scavenging from respiration, body heat, ambulation and sunlight and envision wireless transfer of charge from the storage sites to the nodes. Further, we use model based engineering to evaluate the sustainability of the PVS protocol.

7. **Model based development of Pervasive Health Monitoring Systems** (with demonstration)
   Sandeep Gupta* and Sunit Verma
   Summary: Personal health is a major focus pushing the need for a simple, yet effective method to monitor health. Safety, lifetime, and reliability have been identified as important requirements of medical devices. Failures of these devices are mainly attributed to a mismatch between requirements of Body Sensor Network (BSN) models and their implementations. To counter these problems, we developed Health-Dev, a model-based framework, which abstracts the details between model and implementation to allow design through a high-level specification model, which automatically generates sensor and phone-side code. This demo will demonstrate the ability of user to easily specify different requirements and quickly generate the corresponding code for both the sensor and the smart phone.

8. **MobiCloud: A Secure Mobile Cloud Computing Framework**
   Dijiang Huang* and Tianyi Xing
   Summary: MobiCloud is a secure mobile cloud computing infrastructure that transforms traditional MANETs into a new service-oriented communication architecture. MobiCloud treats each mobile node as a service node, which can be used as a service provider or a service broker according to its capability. In this research, we have established a geo-distributed prototype for MobiCloud with capabilities including resource provisioning, secure storage, resource monitoring and management, and Cloud-based application & services. This project is sponsored by ONR Young Investigator Program.

9. **A Cloud-based Resource and Service Sharing Platform for Computer and Network Security Education**
   Dijiang Huang* and Le Xu
   Summary: A virtual computer and network instructional laboratory (vLab) is established based on cloud computing and Web 2.0 technologies. vLab targets to provide hands-on projects for information assurance education through a remote-access and virtualized laboratory environment that allows students to conduct their course projects without location and time restrictions. vLab has been utilized by many computer science and engineering courses since fall 2011. This project is sponsored by NSF.

10. **SeRViTR - A Secure and Resilient Virtual Trust Routing Framework for Future Internet**
    Dijiang Huang* and Chun-Jen Chung
    Summary: A secure virtualized routing architecture in a global internetworking environment is established in this project. It provides a routing platform that has built-in capability to route traffic with different trustable service requirements and constraints specified by end users. Designs of this virtual routing framework include traffic flow control and control message format based on the programmable OpenFlow network switches. The goal of this project is to enable this virtual trust routing framework to handle both network-centric and user-centric virtual network resource provisioning for future Internet architecture. This project is sponsored by NSF and Japan NICT (National Institution of Information and Communication Technology).

11. Image Tampering Detection

Baoxin Li* and Parag Chandakkar

Summary: One common type of image tampering involves cropping one part of an image and then pasting it to the same or another image by using operations such as resizing, rotation and other distortions, possibly followed by post-processing steps that include blurring the tampered edges to make them look natural. Creating tampered images has become easier with ready availability of digital image processing software. Tampered images may be used to convey falsified information in achieving malicious intentions, which has become a practical issue especially in the age of social media. This has motivated active research on automated detection of image tampering in recent years. In this study, we present a novel approach to this problem. Our approach employs Block Non-Subsampled Contourlet Transform along with Markov Transition Probability Matrix for feature extraction. Then a Support-Vector-Machine-based classifier is trained in the feature space. Experiments were conducted on two commonly-used datasets to evaluate the proposed method, with comparison with a leading existing approach. The results demonstrate that the proposed method outperforms the state of the art by significant margin and at the same time it produces equally good results on both databases.

12. mTrust: Discerning Multi-Faceted Trust in a Connected World

Jiliang Tang, Huiji Gao, Huan Liu*

Summary: Traditionally, research about trust assumes a single type of trust between users. However, trust, as a social concept, inherently has many facets indicating multiple and heterogeneous trust relationships between users. Due to the presence of a large trust network for an online user, it is necessary to discern multi-faceted trust as there are different types of experts. Our study in product review sites reveals that people place trust differently to different people. Since the widely used adjacency matrix cannot capture multi-faceted trust relationships between users, we propose an approach by incorporating these relationships into traditional rating prediction algorithms to reliably infer their strengths. Our work results in interesting findings such as heterogeneous pairs of reciprocal links. Experimental results on real-world data from Epinions and Ciao show that our work of discerning multi-faceted trust can be applied to improve the performance of tasks such as rating prediction, facet-sensitive ranking, and status theory.

13. Scalable Online Surveys with Identity Protection

Guoliang Xue* and Xinxin Zhao

Summary: Most people refuse to participate in online surveys because they are afraid of leaking their private information during the surveys. One solution is to anonymize participants' submissions. Existing solutions are not efficient to work on a large group, e.g. a group containing 10, 000 participants. We propose an anonymous group message submission protocol, which works on a large group. Our protocol guarantees that the submissions are not tampered and the identity of an honest user is preserved.

Sponsor information: This research was supported in part by ARO grant W911NF-09-1-0467 and NSF grant 0901451. The information reported here does not reflect the position or policy of the federal government.

14. Protection of Users' Data Confidentiality in Cloud Computing Systems

Stephen S. Yau* and Ho G. An

Summary: Current cloud computing systems pose serious limitations to protecting users' data confidentiality. Since users' sensitive data is sent in unencrypted forms to remote machines owned and operated by third-party service providers, there are risks of unauthorized use of the

users' sensitive data by service providers. There are many techniques for protecting users' data from outside attackers, but there is currently no effective way to protect users' sensitive data from service providers of the cloud computing systems. In this research, an approach is presented to protecting the confidentiality of users' data from service providers, and ensures that service providers cannot collect users' confidential data while the data is processed and stored in cloud computing systems. Our approach has four major features: (1) separation of software service providers and infrastructure service providers, (2) hiding the information on the owners of data, (3) data obfuscation and (4) software module decomposition and distributed execution.

15. **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 G. An, Yin Yin, and Billibaldo Aranda
    Summary: An overview of our research on design of adaptive service-based software systems (SBS) with security and multiple QoS requirements is presented. This project aims at establishing an approach to developing Adaptive SBS (ASBS), which incorporates QoS monitoring and adaptation (M/A) capabilities in SBS to satisfy multiple QoS requirements. Our overall approach to developing ASBS, including our system modeling approach to constructing Activity-State-QoS (ASQ) models for QoS estimation, techniques for runtime QoS M/A in SBS, and SOA-compliant simulation techniques for validation, are presented. Finally, demonstrations are shown for adaptive resource allocation and QoS-aware security service directory, and an ASBS based on voice communication, motion detection and encryption services, illustrating our research results on QoS optimization based on mixed integer programming, and design of system architecture and distributed M/A modules.

16. **Fine-grained Private Matching for Proximity-based Mobile Social Networking**
    Yanchao Zhang* and Jinxue Zhang
    Summary: Proximity-based mobile social networking (PMSN) refers to the social interaction among physically proximate mobile users directly through the Bluetooth/WiFi interfaces on their smart phones or other mobile devices. It becomes increasingly popular due to the recently explosive growth of smart phone users. Profile matching means two users comparing their personal profiles and is often the first step towards effective PMSN. It, however, conflicts with users' growing privacy concerns about disclosing their personal profiles to complete strangers before deciding to interact with them. We tackle this open challenge by designing a suite of novel fine-grained private matching protocols. Our protocols enable two users to perform profile matching without disclosing any information about their profiles beyond the comparison result. In contrast to existing coarse-grained private matching schemes for PMSN, our protocols allow finer differentiation between PMSN users and can support a wide range of matching metrics at different privacy levels. The security and communication/computation overhead of our protocols are thoroughly analyzed and evaluated via detailed simulations and real implementations.