Sixth Annual Workshop on Information Assurance Research and Education

Information Assurance Center
Arizona State University

Posters

Wednesday, May 1, 2013
1:00 p.m. to 2:00 p.m. & 3:30 p.m. to 4:45 p.m.
Artisan Court, 30 E. 7th Street, Tempe, AZ

1. **A Cloud-based Resource and Service Sharing Platform for Computer and Network Security Education**
   Dijiang Huang*, Le Xu, and Wei-Tek Tsai*
   Summary: In this project, we developed a vLab system, which provides the following features: (a) a reconfigurable networking environment that is capable of creating various types of networks and allows students to experience real-world computer networking and security situations; (2) a collaborative laboratory environment, where individual experimental environments can be shared and allow students to establish a collaborative sharing environment for security testing and penetration testing; (3) a series of progressive hands-on network security experiments are designed by using a 3-phase progressive teaching model. Since the summer of 2011, the vLab has hosted 2892 VMs to serve 604 graduate and 530 undergraduate students across 6 networking courses over 20 hands-on experiments.

2. **Verifying Access Control Properties with Design by Contract**
   Gail-Joon Ahn* and Carlos Rubio Medrano
   Summary: Ensuring the correctness of high-level security properties, including access control policies in mission-critical applications, is indispensable. Recent literature has shown how immaturity of such properties has caused serious security vulnerabilities, which are likely to be exploited by malicious parties for compromising a given application. This situation gets aggravated by the fact that modern applications are mostly built on previously developed reusable software modules and any failures in security properties in these reusable modules may lead to vulnerabilities across associated applications. In this project, we propose a framework to address this issue by adopting Design by Contract (DBC) features. Our framework accommodates security properties in each application focusing on access control requirements. We describe how access control requirements based on ANSI RBAC standard model can be specified and verified at the source code level.

3. **Towards Multi-layered Security for Mediating Inter-Process Communication on Android**
   Gail-Joon Ahn*, Yiming Jing and Hongxin Hu
   Summary: Android, as the most popular smartphone operating systems in the current smartphone market, provides two core security mechanisms, a permission system and

*ASU faculty member

application sandboxing. However, recent studies show that Android is vulnerable to a variety of attacks that could bypass these existing security mechanisms. In this project, we propose a practical multi-layered security framework, called TripleMon, to support policy-based mediation on Android IPC at multiple layers of the Android software stack and mitigate prominent attacks.

4. Using Instruction Sequence Abstraction for Shellcode Detection

Gail-Joon Ahn* and Ziming Zhao

Summary: Although several research teams have focused on binary code injection, it is still an unsolved problem. Misuse-based detection lacks the flexibility to tackle unseen malicious code samples and anomaly-based detection on byte patterns is highly vulnerable to byte cramming and blending attacks. In addition, it is desperately needed to correlate newly-detected code injection instances with known samples for better understanding the attack events and tactically mitigating future threats. In this project, we propose a technique for modeling shellcode detection and attribution through a novel feature extraction method, called instruction sequence abstraction, that extracts coarse-grained features from an instruction sequence. Our technique facilitates a Markov-chain-based model for shellcode detection and support vector machines for encoded shellcode attribution. We also describe our experimental results on shellcode samples to demonstrate the effectiveness of our approach.

5. Exploring Provenance in Social Media

Zhuo Feng, Pritam Gundecha and Huan Liu*

Summary: Social media has profoundly impacted the way people interact and communicate. Although the existing structure of social media allows users to easily create, receive and propagate a piece of information, it provides no mechanism to know more about the received information for its users. In most cases, users even have no basic knowledge about the received information, including the provenance (also known as sources or originators) of information. Provenance knowledge provides additional context to the received information such that a user can assess how much value, trust, and validity should be placed in a received information. We study a novel research problem that facilitates a few known recipients (less than 1% of the total recipients) to seek the provenance of information by recovering how it has flown from its originators. The experimental results show that the proposed mechanism is effective in correctly identifying the additional recipients and seeking the provenance of information.

6. Understanding the Cyber Security Task. A Compilation of Work from Survey and Experimentation

Nancy Cooke*, Shree Jariwala, Prashanth Rajivan and Michael Champion

Summary: Over the past few years we have been able to further our understanding of the human component of cyber security. We have sought to gain an understanding of the motivations, background, and task of the cyber security analyst. In order to do this we conducted a broad overview survey aimed at identifying the demographic information of cyber security analysts. We paired this information with previous cognitive task analyses and applied this information to the development of CyberCog2, a triage-style task environment. Within this experiment, we considered one of the unique components of the human analyst, the value of working as an interdependent team. Within this experiment we found that while low-level tasks were performed at relatively the same level between teams working together

and teams that were not working together, teams that were worked together were able to out perform on complex tasks compared to teams that were not working together. This result shows a definitive argument for working together within cyber triage related tasks.

7. **A Framework of Skyline-Join Operators for Static and Stream Environments in Information Assurance Applications**
   Mithila Nagendra and K. Selcuk Candan*
   Summary: Efficient processing of skyline queries has been an area of growing interest for decision making in static and stream environments. Most existing static and streaming techniques assume that the skyline query is applied to a single data source. Unfortunately, this is not true in many information assurance applications in which the skyline query may involve attributes belonging to multiple data sources. We introduce SkySuite. a framework of skyline-join operators that can be leveraged to efficiently process skyline-join queries over both static and stream environments. Among others, SkySuite includes (1) a novel Skyline-Sensitive Join (SSJ) operator that effectively processes skyline-join queries in static environments, and (2) a Layered Skyline-window-Join (LSJ) operator that incrementally maintains skyline-join results over stream environments.

8. **DBN: Leveraging Approximate Functional Dependencies for Efficient Tensor Decompositions to Support Decision Making in Information Assurance Applications**
   Mijung Kim and K. Selcuk Candan*
   Summary: : For many information assurance applications involving analysis of multi-dimensional data sets for decision making, it is necessary to have efficient tensor and relational operations. Two widely used tensor decompositions, CP and Tucker, are proven to be effective in multi-aspect data analysis. Since the number of modes of the tensor data is one of the main factors contributing to the cost of the tensor operations, we focus on reducing the modality of the input and propose a novel decomposition-by-normalization scheme that first normalizes the given relation into smaller tensors based on the functional dependencies of the relation and then performs the decomposition using these smaller tensors. The decomposition and recombination steps of the decomposition-by-normalization scheme fit naturally in settings with multiple cores.

9. **STFMap: Query- and Feature-driven Visualization of Large Time Series Data Sets for Information Assurance Applications**
   Xiaolan Wang, Rosaria, Rossini, K. Selcuk Candan*, and Maria Luisa Sapino
   Summary: Since many information assurance applications rely on time-based data, helping experts explore large time series data sets is critical. In this interactive system preview, we argue that time series often carry structural features that can, if efficiently identified and effectively visualized, help reduce visual overload and help the user quickly focus on the relevant data. Relying on this observation, we introduce a novel STFMap system, which includes four innovative query- and feature-driven time series data set visualization techniques: (a) segment-maps, (b) warp-maps, (c) stretch-maps, and (d) feature-maps. These rely on the salient temporal features of the time series and their alignments with respect to the given user query to help users explore the data set in a query-driven fashion.

10. **Risk Assessment Using TVA Analysis for Balancing Risk Mitigation and System Support**
    Roberto Mejias*

Summary:
Information security risk assessment must determine the vulnerability of key information resources against cyber-attacks. This is challenging when organizations possess a wide range of IT resources, but are unsure which IT safeguards are most effective against the most probable cyber attacks. The TVA (Threat-Vulnerability-Asset) worksheet is an effective risk analysis tool that provides a comprehensive methodology that (a) identifies the key IT resources supporting critical operations, (b) identifies the most probable cyber-attacks against those critical IT assets, (c) uses the TVA Worksheet template to assesses which current IT controls should prevent identified cyber-threats, and (d) identifies remaining vulnerabilities (residual risk), and which IT controls to reduce/deter cyber-attack vulnerability. One of the persistent issues in risk assessment research is to determine which IT controls and safeguards protect which key IT resources from the most probable cyber attacks.

11. An Approach to Proactive Malware Defense

Stephen S. Yau* and Arun Balaji Buduru

Summary: Most malware defense techniques are signature-based, and hence are reactive, i.e. only the malwares with similar signatures with some known malwares' signatures can be detected. Malwares, such as "Eurograbber", a modified Zeus botnet, remained undetected for a long time because its signature is not similar to those of any known malwares. On the other hand, most of heuristics-based malware detection techniques are ineffective because they lack good ways of generating meaningful heuristics. We plan to develop a three-pronged strategy utilizing machine learning and planning techniques to detect and prevent malwares with signatures not similar to those of any known malwares from damaging critical system assets. Our approach will automate the detection, analysis and prevention processes in malware defense, and reduce the delay between malware detection and prevention, and the need for human interventions in malware defense.

12. CloudAssure: A Framework for Generating Data Transfer Decisions for Cloud Systems

Stephen S. Yau*, Arun Balaji Buduru, David Lucero and Jeremy Wright

Summary: Data leakage is very damaging to organizations, especially to those dealing with highly sensitive data. Between 2008 and 2009, American businesses alone had more than $1 trillion in intellectual property damages due to cyber attacks. However, the problem of data leakage so far has no effective solution. We plan to develop a system framework, called CloudAssure, for assisting users/nodes in dynamic networks to make proper decisions on sensitive data transfers. CloudAssure generates recommendations to the sender of the sensitive data whether the send would allow sensitive data transfers among the nodes/users in volatile networks, based on the probabilities of any leakages of sensitive data as a result of the transfers. The use of a three-stage process along with an MDP for generating recommendations will allow CloudAssure to operate dynamically and adapt to changes in the datasets and hierarchical users/nodes' privilege structure.

13. Automated Composition of Secure and Adaptive Workflows in Mobile Cloud Environments

Stephen S. Yau* and Dazhi Huang

Summary: This project is to develop an approach for automated composition of secure and adaptive workflows in mobile cloud environments to provide trustworthy software applications for users. This approach will have three parts: (1) Application developers generate and publish "blueprints" (specifications) of workflows in a "workflow store" based

on workflow goals and constraints. (2) Mobile users discover proper "blueprints" of workflows in the "workflow store", and provide their own customization requirements. (3) An agent synthesizer automatically synthesizes secure and adaptive workflow agents for executing the workflows based on the discovered "blueprints", customization requirements, and resource availability. Among the three parts, the agent synthesizer in (3) will be our research focus, while existing tools and techniques will be exploited and adapted for (1) and (2).

14. Unobservable Active Authentication for Smartphones

Lingjun Li, Xinxin Zhao, and Guoliang Xue*

Summary: Smartphones usually store some of their owners' private information, which causes a great loss to the owners if it is accessed by an unwanted party. To reduce such a loss, it is necessary to design a mechanism for smartphones to authenticate the current users. Such a mechanism can help inhibit smartphone theft and safeguard the information stored in smartphones. In this project, we propose a novel biometric-based system to achieve continuous and unobservable authentication for smartphones. The system uses a classifier to learn the owner's finger movement patterns and actively checks the current user's finger movement patterns against the owner's. The system continuously authenticate the current user without interrupting user-smartphone interactions. Experiments show that our system is efficient on smartphones and achieves high accuracy.

15. Trust Establishment via Privacy-Preserving Spatiotemporal Matching

Yanchao Zhang* and Jingchao Sun

Summary: The explosive growth of mobile-connected and location-aware devices makes it possible to have a new way of establishing trust relationships, which we coin as spatiotemporal matching. In particular, a mobile user could very easily maintain his spatiotemporal profile recording his continuous whereabouts in time, and the level of his spatiotemporal profile matching that of the other user can be translated into the level of trust they two can have in each other. Since spatiotemporal profiles contain very sensitive personal information, privacy-preserving spatiotemporal matching is needed to ensure that as little information as possible about the spatiotemporal profile of either matching participant is disclosed beyond the matching result. We propose a cryptographic solution based on Private Set Intersection Cardinality and a more efficient non-cryptographic solution involving a novel use of the Bloom filter. We thoroughly analyze both solutions and compare their efficacy and efficiency via detailed simulation studies. This research is sponsored by National Science Foundation.