Symposium on
Information Assurance Research and Education

Information Assurance Center
Arizona State University

Poster Session

Thursday, October 16, 2014
12:40 p.m. to 2:00 p.m. & 4:00 p.m. to 5:00 p.m.
Ballroom Ventana C, Memorial Union, Tempe, AZ

1. **Towards Federated Attribute-based Access Control in ESnet**
   Gail-Joon Ahn* and Carlos E. Rubio-Medrano
   Summary: Attribute-based access control (ABAC) has been regarded in recent years as an effective way for providing security guarantees in collaboration environments, due to its alleged flexibility and efficiency for meeting the access control requirements of heterogeneous organizations. Despite the growing interest in ABAC, there still need consensus on a reference model that comprehensively describes all necessary components and functions, in such a way non-trivial security properties can be effectively taken into account. In order to overcome this limitation, we propose an abstract model that includes a precise definition of attributes and relevant core components. In addition, we introduce the notion of security tokens that serve as a layer of association between attributes and access rights. We also articulate how our approach can be applicable to DoE's network environment called ESNet.

2. **Forensic Analysis on Mobile Devices**
   Gail-Joon Ahn*, Adam Doupe* and Jeremy Whitaker
   Summary: Allowing mobile devices to connect to corporate networks poses a significant security risk such as data loss, data theft, malware-infected networks, password compromises and more. The way in which MDM solutions allow mobile devices access to corporate networks, applications and data fails to adequately manage mobile device risk. Mobile security requires a comprehensive assessment of the risk comprising network, device and applications before granting access. Existing MDM solutions fall short of addressing a wide spectrum of mobile risks, which are dynamic in nature and cannot be addressed without forensic-driven analysis and the advanced forensic capability. In this project, we seek a comprehensive approach to discover abnormal characteristics and attack attributions including usage patterns and application attributes. Such characteristics will allow us to further investigate and propose a framework for identifying anomalies and potential compromises in the mobile-centric network infrastructure.

*ASU faculty member

3. Automated Risk Assessment of Mobile Applications

Gail-Joon Ahn*, Adam Doupe* and Yiming Jing

Summary: Mobile operating systems, such as Apple's iOS and Google's Android, have supported a ballooning market of feature-rich mobile applications. However, helping users understand security risks of mobile applications is still an ongoing challenge. While recent work has developed various techniques to reveal suspicious behaviors of mobile applications, there exists little work to answer the following question: are those behaviors necessarily inappropriate? In this project, we seek an approach to cope with such a challenge and present a continuous and automated risk assessment framework called RiskMon that uses machine-learned ranking to assess risks incurred by users' mobile applications, especially Android applications. RiskMon combines users' coarse expectations and runtime behaviors of trusted applications to generate a risk assessment baseline that captures appropriate behaviors of applications. With the baseline, RiskMon assigns a risk score on every access attempt on sensitive information and ranks applications by their cumulative risk scores.

4. Policy-Driven Security Management for Fog Computing

Gail-Joon Ahn*, Adam Doupe*, Clinton Dsouza and Marthony Taguinod

Summary: With the introduction and rising use of mobile devices, the Internet of Things (IoT) has recently received considerable attention since the IoT has brought physical devices and connected them to the Internet, enabling each device to share data with surrounding devices and virtualized technologies in real-time. Consequently, the exploding data usage requires a new, innovative computing platform that can provide robust real-time data analytics and resource provisioning to clients. As a result, fog computing has recently been introduced to provide computation, storage and networking services between the end-users and traditional cloud computing data centers. This project proposes a policy-based management of resources in fog computing, expanding the current fog computing platform to support secure collaboration and interoperability between different user-requested resources in fog computing.

5. Title: Building Robust Firewalls for Software-Defined Networks

Gail-Joon Ahn*, Adam Doupe* and Wonkyu Han

Summary: Software-Defined Networking (SDN) introduces significant granularity, visibility and flexibility to networking, but at the same time brings forth new security challenges. One of the fundamental challenges is to build robust firewalls for protecting OpenFlow-based networks where network states and traffic are frequently changed. To address this challenge, we introduce FLOWGUARD, a comprehensive framework, to facilitate not only accurate detection but also effective resolution of firewall policy violations in dynamic OpenFlow-based networks. FLOWGUARD checks network flow path spaces to detect firewall policy violations when network states are updated. In addition, FLOWGUARD conducts automatic and real-time violation resolutions with the help of several innovative resolution strategies designed for diverse network update situations. We also implement our framework and demonstrate the efficacy and efficiency of the proposed detection and resolution approaches in FLOWGUARD through experiments with a real-world network topology.

6. **Graphical Representation of Security Settings in Android**

Aaron Gibson and Rida Bazzi*

Summary: On many personal devices, security settings are represented in a hard-to-comprehend way. On Android, the focus of this research, existing security requires apps to register permissions for access to sensitive resources. The user approves permissions which allow the apps access to sensitive resources. Such permissions are presented as a long list which the average user has neither the knowledge nor the patience to approve. This is further compounded by the fact that permissions are an incomplete mechanism to ensure secure access to resources. Furthermore, permissions do not always track flows of information from the apps, which are often at odds with the user's expectation of what they have access to. Our proposed research seeks to identify and visualize the types of information that flow between applications. Using this information, we plan on creating new security policies that are more comprehensive to security as well as more intuitive to the user.

7. **DEXTAR: A Cyber Security Testbed**

Nancy Cooke*, Steve Shope (Sandia Research Corporation), Aaron Bradbury and Michael Champion (University of Greenwich)

Summary: Closing the gap between the human and the computer in an effort to create a more resilient and responsive system to defend our networks and data is an on-going effort that is being tackled by scientists and researchers from all sides. Advancements in both areas, while beneficial, cannot be fully realized unless both areas can come together in advanced testing environments that can leverage full-scale operations, time sensitive measurements, and performance evaluation of both the human and the system. The DEXTAR cyber testbed supports human-in-the-loop testing of cyber security tools or training solutions. This poster will highlight the components and capabilities of this system and present future areas of work. This work is sponsored by the Army Research Office.

8. **SDNIPS: Enabling Software-Defined Networking Based Intrusion Prevention System in Clouds**

Tianyi Xing, Zhengyang Xiong, Dijiang Huang* and Deep Medhi

Summary: Security has been considered as one of the top concerns in clouds. Intrusion Detection and Prevention Systems (IDPS) have been widely deployed to enhance the cloud security. However, none of existing works established a comprehensive IPS solution to reconfigure the cloud networking environment on-the-fly to counter malicious attacks. In this paper, we present an SDN-based IPS solution called SDNIPS that is a full lifecycle solution including detection and prevention in the cloud. We propose a new IDPS architecture based on Snort-based IDS and Open vSwitch (OVS). We also compare the SDN-based IPS solution with the traditional IPS approach from both mechanism analysis and evaluation. Network Reconfiguration (NR) features are designed and implemented based on the POX controller to enhance the prevention flexibility. Finally, evaluations of SDNIPS demonstrate its feasibility and efficiency over traditional approaches.

9. **Investigating Human Factors in Image Forgery Detection**

Baoxin Li* and Parag Chandakkar

Summary: In the age of social media, one can find an enormous volume of forged images on-line. These images have been used in the past to convey falsified information and achieve harmful intentions. While creating forged images has become easier due to software

advancements, there is no automated algorithm which can reliably detect forgery. Human performance is still the gold-standard for this task. We conduct a subjective evaluation test with the aid of eye-tracker to investigate into human factors associated with this problem. We compare the performance of an automated algorithm and humans for forgery detection problem. We also develop an algorithm which uses the data from the evaluation test to predict the difficulty-level of an image1. The experimental results presented in this paper should facilitate development of better algorithms in the future.

10. Exploring Personal Attributes from Publicly Available Interactions to Secure Users' Privacy

Pritam Gundecha, Jiliang Tang and Huan Liu*

Summary: The recent study suggests that many personal attributes are predictable providing users' personal data. To address these privacy concerns, users are usually left with profile settings to mark some of their personal data invisible. However, users often interact with others using publicly administered posts (Facebook page, for example). Although the aim of such interactions is to help users to become more social, visibilities of these interactions are beyond their profile settings and publicly accessible to everyone. The focus of this work is to explore such unprotected and publicly available interaction data so that users' are well aware of these new vulnerabilities and adopt measures to mitigate them further. In particular, we ask - are users' personal attributes predictable using only publicly available interactions? To answer this question, we design a novel framework to show the predictability of users' personal attributes with public interactions.

11. Malware Task Identification: A Functional Cognitive Modeling Approach

Christian Lebiere (CMU), Paulo Shakarian* (ASU), Stefano Bennati (CMU), Robert Thomson (CMU) and Eric Nunes (ASU)

Summary: Malware reverse-engineering is an important type of analysis in the domain of cyber-security. Rapidly identifying the tasks that a piece of malware is designed to perform is an important part of reverse engineering that is manually performed in practice as it relies heavily on human intuition. In this paper, we present an automated approach to malware task identification using ACT-R cognitive models. Using a real-world malware dataset, these cognitive models identified sets of tasks with an unbiased F1 measure of 0.94 – significantly out-performing baseline approaches. Even when trained on historical datasets of malware samples from different families, the cognitive models still maintained the precision of baseline methods while providing a significant improvement to recall (identifying over 60% of malware tasks).

12. Host Based Detection of Advanced MiniDuke Style Bots in Smartphones through User Profiling

Vishnu Kilari, Guoliang Xue* and Margaret Todd

Summary: Smartphones are a ripe attack space for malware producers, particularly bot masters. Bots require communication with the bot master to perform their flexible and dynamic attacks, but this communication with command and control (C&C) is also a botnet's weakness. There is an arms race between attackers and defenders with respect to obfuscating and detecting a bot's connection to C&C, such as using Domain Generation Algorithms (DGA) and using encryption, stenography or obfuscation to hide within legitimate Online Social Networks (OSNs) such as Twitter, Facebook, Baidu and Reddit. We propose a novel C&C channel that would not be detected by current methods by combining these approaches

to use a User Generation Algorithm (UGA) with public key encryption to protect the botnet from sabotage, and simultaneously create a detection system for such bots.

13. Adaptive Touch Screen based probabilistic user Re-authentication

Stephen S. Yau* and Arun Balaji Buduru

Summary: Increasingly more confidential information is being stored and/or viewed on smart devices. Furthermore, rising BYOD (Bring Your Own Device) trend across the market is leading to storage of enterprise data on personal smart devices. Currently, most or all of the smart phones employ four to six digit or pattern-based one-time user authentication schemes, which is clearly not enough because attacker can easily brute force them or can keep the authenticated session open on physically compromised smart device until all the confidential data are extracted. Most of the existing re-authentication techniques use centralized architecture and require servers to train and update the learning model used for user re-authentication. Hence, we develop an approach to eliminating or reducing the use of centralized servers. Our approach includes grid value generation algorithm to estimate importance of grids/states and Markov Decision Process (MDP) algorithm to re-authenticate user gesture with probabilistic user gesture model.

14. An effective resource optimization approach through stochastic planning of IoT resources in smart environments

Stephen S. Yau* and Arun Balaji Buduru

Summary: IoT (Internet of Things) is increasingly becoming more popular mainly due to the fact that almost all the smart devices nowadays are network-enabled to facilitate many current and emerging applications. However, some important issues still need to be addressed before fully realizing the potential of IoT applications. One of the most important issues is to have effective approaches to planning various device actions to satisfy user requirements efficiently and securely in mobile IoT applications. In this type of systems, mobile networks with elastic resources from various mobile clouds are effective to support IoT applications. We present an effective approach to intelligent planning for mobile IoT applications. This approach includes a learning technique for dynamically assessing the user's mobile IoT application and an MDP (Markov Decision Process) planning technique for enhancing efficiency of IoT device action planning. Simulation results are presented to show the effectiveness of our approach.

15. Your Song Your Way: Rhythm-Based Two-Factor Authentication for Multi-Touch Mobile Devices

Yimin Chen and Yanchao Zhang*

Summary: Multi-touch mobile devices have penetrated into everyday life to support personal and business communications. Secure and usable authentication techniques are indispensable for preventing illegitimate access to mobile devices. This work is to develop RhyAuth, a novel two-factor rhythm-based authentication scheme for multi-touch mobile devices. RhyAuth requires a user to perform a sequence of rhythmic taps/slides on a device screen to unlock the device. The user is authenticated and admitted only when the features extracted from her rhythmic taps/slides match those stored on the device. RhyAuth is a two-factor authentication scheme that depends on a user-chosen rhythm and also the behavioral metrics for inputting the rhythm. Our preliminary results on Android devices show that RhyAuth is highly secure against various attacks and also very usable for both sighted and visually impaired people. This work is supported by NSF.