Annual Symposium on Information Assurance Research and Education

Information Assurance Center
Arizona State University

Poster Session

Friday, November 13, 2015
12:40 p.m. to 1:40 p.m. & 4:00 to 5:00 p.m.
Ballroom Ventana C, Memorial Union
Arizona State University, Tempe, AZ

1. **Threat Intelligence Analytics (TIA): Assembling the Jigsaw Puzzles of Cybercrimes**
   Anupam Panwar, Ajay Modi, Kyungyong Han, Kevin Lao, Daniel Martin, Sajid Anwar, Jangwon Yie and Wonkyu Han, Ziming Zhao*, Adam Doupé* and Gail-Joon Ahn*

   Summary: Over the past few years, the volume and frequency of new cyber threats and variants targeting both the private and the public sector have exploded and become critical concerns. A staggering number of cybercrimes that evade existing security measures have complicated workflows and involve multiple criminals and organizations. However, current threat analysis and intelligence discovery are performed piecemeal in an ad-hoc manner. For example, a modern malware analysis system can dissect a piece of malicious code by itself. But, it cannot automatically identify the criminals who developed it or relate cyber attack events with it. Consequently, it is imperative to automatically assemble the Jigsaw puzzles of a cybercrime by performing holistic threat intelligence analytics on data collected from heterogeneous sources, such as malware, underground social networks, cryptocurrency transaction records, etc. With this in mind, we propose a framework called *threat intelligence analytics* (TIA) that considers all sorts of threat sources as a whole and performs collective analysis across different threat sources to discover meaningful knowledge and intelligence related to cybercrime events. The goal of TIA is to provide both the private and the public sector with a trusted platform, where they can safely share their collected threat evidence data through structured specification and protocols, and obtain multi-dimensional threat intelligence generated from TIA. To this end, TIA is designed as a modular framework with RESTful interfaces to glue reusable analytic and data components together. The brain of TIA is a set of algorithms that orchestrate all components and the workflow of intelligence discovery by deciding how to use intelligence generated by components.

2. **Mobile and Web Vulnerability Analysis**
   Sowmya Myneni, Vikranth Doosa, Shravan Purohit, Sai Chandramouli, Yeganeh Safaeisemmani and Yiming Jing, Adam Doupé* and Gail-Joon Ahn*

   Summary: Smartphones and the World Wide Web govern many aspects of our daily lives. Therefore, it is critical to find and discover potential vulnerabilities in real-world mobile applications (apps) and web pages before hackers use them to steal personal information.

---

*ASU faculty member , **Non-ASU faculty member*/researcher

Using parallel computing techniques, we crawled the Web and the Google Play Store for web vulnerabilities. One of these aspects of our research is analyzing real-world Android apps to understand how permissions are distributed among them, and more importantly how they are distributed in different categories of apps. Permissions play an important role in app security as over privileged apps can be exploited by a malicious app to leverage the privileged app's permissions. Most research on Android apps focus on only the most popular apps, while we are examining a wide range of apps: our dataset includes 1.5 million real-world Android apps, crawled from the Google Play Store. Moreover we closely explored the "middle class" of apps (the apps falling in 100 to 500 number of installs), and we found that they are as influential as the rest of the apps in the market because their total install numbers are one third of the rest of the marketplace. The other aspect of our vulnerability analysis research focuses on web vulnerability analysis, particularly on email header injection. We crawled the web to look for those vulnerable web pages, and to find out whether this vulnerability is widespread, and if so, how wide is the impact. Because this vulnerability can be exploited to inject additional email headers and/or modify existing email headers, we are trying to find the correlation between the vulnerable websites with those that are responsible for spamming attacks.

3. Towards Forensics for Web Thin Clients

Mike Mabey and Jeremy Whitaker, Ziming Zhao*, Adam Doupé* and Gail-Joon Ahn*

Summary: Researchers have developed forensic analysis techniques for so many types of digital media that there's a procedure for almost everything a law enforcement officer may encounter at a crime scene. But a new type of device has started to gain momentum in the consumer market: web thin clients. These devices are so different from other types of computing and storage devices that virtually all of the techniques forensic examiners and researchers typically use do not apply, requiring the development of new techniques tailored to their unique attributes. In this work, we present an overview of our approach to extracting residual evidence stored on web thin clients as well as our method for identifying which extensions are installed on an encrypted file system.

4. Exploring Innovative Approaches for Moving Target Defense

Josie Lamp, Marthony Taguinod, Faris Kokulu and Carlos Rubio-Medrano, Ziming Zhao*, Adam Doupé* and Gail-Joon Ahn*

Summary: Recently, *moving target defense* (MTD) has attracted considerable attention from both academia and industry as an innovative paradigm to provide security measurements in computer-based systems. Opposed to traditional approaches, which assume the security configuration of a protected system remains *immutable* during its lifetime, MTD relies on more *proactive* strategies intended to deliberately *modify* such configurations in an effort to significantly *reduce* the probabilities of carrying on a successful attack, without affecting the overall *functionality* of the system. As an example, web applications are considered a critical component of the security ecosystem as they are often the “front-door” for many companies. As a result, vulnerabilities in web applications allow hackers’ access to companies’ private data, in addition to allowing them the opportunity to perform reconnaissance and execute attacks at their own leisure. We seek to use MTD to remove this advantage by introducing diversity to each layer of the web application in order to create effective defense layers. In doing so, we attempt to reduce the chances of attacks, such as remote code executions, by

changing the language and dialect implementations while retaining the underlying functionality of the web application. In addition, we are working on an MTD-based approach tailored for *attribute-based access control* (ABAC), a trending approach for specifying rich and flexible policies that mediate access to sensitive resources, e.g., private data. Using MTD, we aim to *randomly* mutate ABAC policies by adding or removing attributes that belong to end-users, protected resources, and running environments, in an effort to decrease the chances of a successful attack, e.g., bypassing the original policy, while still preserving important security properties, e.g., *who* is allowed to access *what* and under *which* circumstances.

5. Caller ID Spoofing and Spam Calls

Huahong Tu (Raymond) and Gerard Lawrence Pinto, Ziming Zhao*, Adam Doupé* and Gail-Joon Ahn*

Summary: Caller ID spoofing perpetuates and enables voice scams and spams, which cost United States consumers $8.6 billion annually. The FTC has received over 22 million complaints of unwanted (and illegal) voice and voicemail spam. Voice and voicemail spammers are leveraging technical advances in the telephony system that reduce costs and ease spamming. Given that anti-spam techniques and approaches are effective in the email domain, the question we address is: what are the effective defenses against spam calls? In addition, we investigate a systematic framework to understand various techniques and articulate potential countermeasure to prevent such critical challenges.

6. Cyber Security brings Humans in the Loop

Nancy Cooke*, Aaron Bradbury, Jim Blythe, Sarah Kusumastuti, Steven Shope, Jessica Twyford

Summary: With cyber security increasing in relevance, researchers at ASU, USC, and SRC have come together to develop a high fidelity environment where cyber defense research can be conducted with humans in the loop. This multi-university testbed affords team cognition, user interface and design, and other human factors research, along with large-scale and customizable virtual networks where cyber security can be fully simulated. Pilot testing began on 10/22/2015 of an experiment that will examine the ways network analyst teams work together to recognize and resolve cyber attacks in this new environment.

7. fSense: Financial Fraud Detection via Visual Analytics

Mehmet Yigit Yildirim, Selcuk Candan*, Hasan Davulcu*

Summary: Today, in order to obtain a single unified view of fraud activity across the enterprise and manage fraud on a cross-institution basis fraud detection companies collect, verify and analyze real-time consumer data and financial information. Synthetic identity theft occurs when thieves create new identities either by combining real and fake identifying information to establish new accounts with fictional identities, or create a brand new identity from fake or inaccurate information. Synthetic identity theft is the fastest growing type of ID fraud in the U.S. Detecting increasingly complex fraud schemes (such as sythetic ID's and identity theft) require the ability to integrate and enrich data from private financial sources with relevant public data sources and hunt for recurring and interconnected anomalous patterns. The objective of this project is to develop a real-time data integration and pattern

analysis platform, called fSense, to support smart complex financial patterns (CFP) discovery and fraud decision services.

8. Attribute-Based Cryptography for Attribute-Based Access Control

Zhijie Wang, Dijiang Huang*

Summary: Attribute-Based Encryption (ABE) defines user's identity as a set of attributes, and messages can be encrypted with respect to subset of attributes or policies defined over set of attributes. Users should only be able to decrypt a ciphertext if this person holds a key for matching attributes. Attributes Based Access Control (ABAC) allows a simple expression of a rich, complex access control policy whereby access rights are granted to users with proper attributes (e.g., user attributes, resource attributes, environment attributes). We proposed various ABE cryptographic algorithms for privacy preservation and better performance in terms of computational and communication cost. To address the conversion from RBAC to ABAC, an attribute lattice approach for ABE was introduced to define a senior relation among all values of an attribute. We further study attribute revocation, hierarchical attributes, trust authority delegation and federated operations. we will investigate into the security and privacy policy management framework using ontology-based approaches to coordinate security policies among multiple administrative domains. Finally, we will investigate into the ABE-enabled ABAC and how to use it for various DoD application scenarios.

9. Secured and Resilient Networking (SRN)

Ankur Chowdhary, Dijiang Huang*

Summary: Current enterprise datacenter environments lack orchestrated and resilient defensive mechanism based on quantifiable metrics and evaluation methods. Secured and Resilient Networking (SRN) based defense mechanism plans to address this issue via programmable and dynamic defensive mechanisms. Project also plans to achieve Moving Target Defense (MTD) using attack prevention and mitigation in timely and intelligent fashion. To achieve MTD, attack tree/graph based security quantification and analysis is used. Some research challenges addressed as part of the project are described below: (1) Traditionally attack graph generation and representation has scalability issues because of a large number of network nodes, topology changes and new vulnerabilities. SRN framework plans to use a parallel computing framework such as Hadoop and Spark to address scalability issues. (2) Alert Correlation Graph to correlate attacker behavior and alert analyzer to analyze the alert. (3) Intelligent way of selecting Attack Countermeasure based on recommendations from Adaptive Secure Traffic Engineering Module (ASeTE). (4) Cost of applying countermeasure and benefit is evaluated using benefit and ROI metrics. Also the virtual machine state is analyzed prior to countermeasure and post countermeasure application using Virtual Machine Security Index(VSI).

10. Brew: A Conflict Free Policy Implementation For Distributed SDN Environments

Sandeep Pisharody and Dijiang Huang*

Summary: Separation of network control from devices in Software Defined Network (SDN) allows for easy centralized management and implementation of security policies in a distributed environment. The ease of programmability in SDN makes it a great platform for

Moving Target Defense (MTD) initiatives. Effective implementation of countermeasures in a Moving Target Defense (MTD) scenario could result in dynamic change of network topology, or host reconfiguration. Verifying the adherence of these new flow policies to security policies and ensuring flow rule consistency is especially challenging especially in distributed environments where the distribution scheme for SDN controllers affects the hardness of this problem. Our framework, Brew, ensures that in a large scale SDN implementation with distributed controllers, any MTD countermeasure actions do not lead to flow rule conflicts and seeks to provably verify that the post-MTD countermeasure flow rules adhere to the security policy, thereby ensuring a consistent conflict-free security policy.

11. Toward Bot Detection in Social Media

Tahora H. Nazer, Fred Morstatter, Liang Wu, Huan Liu*

Summary: Bots have become a prominent issue in social media as they own a large portion of accounts and produce massive amount of content. They can perform malicious tasks such as influencing discussions and inflating popularity of celebrities and hence need to be detected. Removing a normal user from the network might cause dissatisfaction and most detection methods are too conservative in reporting a user as a bot which results in mass existence of them in social media. In this work we focus on increasing the number of bots being detected without drastically decreasing the accuracy. Towards this goal, we have collected two datasets based on two different algorithms from Twitter and our experiments have shown promising results.

12. Toward Trustworthy Information Detection with Social Status Analysis

Liang Wu, Xia Hu, Huan Liu*

Summary Understanding public opinions with social media has recently received considerable attention. The underlying assumption of traditional methods is that online accounts are equally helpful, which could spoil the analysis since the quality of content from different users varies drastically from excellent to spam. Social media, in addition to the content, provides valuable non-content information such as links between accounts and user behaviors. The focus of this work is to explore how the heterogeneous social media data can be exploited to estimate the information quality. In particular, we design a comprehensive framework to find high-quality information sources. Experimental results prove that the framework is effective in facilitating current and emerging social media applications.

13. Cyber-Deception and Attribution in Capture-the-Flag Exercises

Eric Nunes, Paulo Shakarian*

Summary: Attributing the culprit of a cyber-attack is widely considered one of the major technical and policy challenges of cyber-security. The lack of ground truth for an individual responsible for a given attack has limited previous studies. Here, we overcome this limitation by leveraging DEFCON capture-the-flag (CTF) exercise data where the actual ground-truth is known. In this work, we use various classification techniques to identify the culprit in a cyberattack and find that deceptive activities account for the majority of misclassified samples. We also explore several heuristics to alleviate some of the misclassification caused by deception.

14. Protecting Critical Cloud Infrastructures with Predictive Capability

Arun Balaji Buduru, Vinjith Nagaraja, Stephen S. Yau*

Summary: Emerging trends in cyber system security breaches, including those in critical infrastructures involving cloud systems, have shown that attackers have abundant resources, including both human and computing power, to launch attacks. In order to have much better protection for critical cloud infrastructures, effective approaches with predictive capability are needed. Much research has been done by applying game theory to generating adversarial models for protecting critical infrastructures. However, these approaches have serious limitations, some of which are due to the assumptions used in these approaches, such as rationality and Nash equilibrium, which may not be valid for current and emerging cloud infrastructures. Another major limitation of these approaches is that they do not capture probabilistic human behaviors accurately. In order to greatly improve the protection of critical cloud infrastructures, an approach is being developed to predicting security breaches in critical cloud infrastructures with accurate system-wide causal relationship and probabilistic human behaviors.

15. Predicting Risky Behavior(s) in Individual Patients in IoT Environment

Arun Balaji Buduru, Stephen S. Yau*, Zeno Franco**, Ahamed Sheikh**

Summary: Serious mental behavior (MH) problems have caused estimated loss of $317B nationally in annual healthcare expenditures, lost productivity, and disability benefit payments. MH problems are correlated with cardiovascular disease, diabetes and early mortality. In addition, access to appropriate MH treatment and prevention services are not always readily available. The objective of this project is to predict the risky behaviors of users based on their emotional states and complex activities which include both internal emotions, such as stress or depression, and externally exhibited emotions, such as angry outbursts, damage to property or involving verbal abuse or altercation. This prediction is accomplished by probabilistic capturing and analyzing of various types of risky behaviors exhibited by users, which are observed through real-time data acquisition from users in their IoT environments.

16. Un-Aware Biometric Authentication of Users with Body-area Devices in IoT Environments

Adel Alshamrani, Arun Balaji Buduru, Stephen S. Yau*

Summary: One of the major difficulties of having effective applications of IoT-based systems is to provide security protection to the application systems, especially in un-aware user authentication. The main objective of this project is to authenticate the users without their intentional inputs using their body-area devices in the application systems. This is especially important to ensure that authorized body-area devices read data from the legitimate user. Our approach is based on data extraction and transformation, fusing transformed data from various body-area devices, and extracting relevant features. The extracted features can then be used to efficiently discriminate and effectively authenticate the users.